完全隐藏策略的基于属性可搜索加密方案

许盛伟[1,2]，王荣荣[1,2]，赵　海[1,2]

(1. 北京电子科技学院，北京 100070; 2. 西安电子科技大学 通信工程学院，西安 710071)

摘　要：目前的基于属性可搜索加密方案（ATT-PEKS），虽然解决了关键词密文只能被唯一用户搜索的限制，实现了加密数据的多用户共享，但是却没有隐藏访问策略，访问策略一旦被不好奇且不可信赖的服务器攻击者获取到，可能会造成机密信息的泄露。所以，为了解决此问题，提出了完全隐藏策略的基于属性可搜索加密方案，并给出了具体的算法构造，使得方案不仅具有多用户数据共享的优势，还实现了访问策略的完全隐藏。并对此方案进行了安全性以及性能分析，证明了方案具有在属性集合模型下的抗攻击性安全，还能保证索引和关键词明文的机密性。在性能方面使用较少的运算量就可以实现隐藏访问策略和加密数据共享两大功能。

关键词：基于属性；可搜索加密；隐藏访问策略；数据共享

中图分类号：TP309.7　　doi: 10.3969/j.issn.1001-3695.2017.12.0857

Attribute-based encryption scheme with fully hidden access structure

Xu Shengwei[1, 2], Wang Rongrong[1, 2], Zhao Hai[1, 2]

(1. *Beijing Electronic Science & Technology Institute*, *Beijing* 100070, *China*; 2. *School of Telecommunications Engineering*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: The current　Attributa-based public encryption with keyword search(ATT-PEKS) , although it solves the problem that the keyword ciphertext can only be uniquely searched by the user to enable multi-user share of encrypted data, it does not hide the access structure. Once the access structure is obtained by unreliable servers attackers, it may be exposed to confidential information. Therefore, in order to solve this problem, this paper proposed an attributa-based public encryption scheme with keyword search that completely hides the access structure, which not only preserved the advantages of ATT-PEKS to realize multi-user data sharing, but also realized the complete concealment of the access structure that prevents the policy information leaking. And it analyzed the security and performance of the scheme. The simulation game proves that the scheme has the anti-attack security under the attribute set model, and also ensures the confidentiality of the index and the key words. The use of less computing power in terms of performance can be achieved hidden access policies and encrypted data sharing two functions.

Key words: based on the attribute; searchable encryption ; hidden access structure; data-sharing

0　引言

在数据爆炸的当今社会，数据存储和共享的问题在云技术的来临后而得到了很好的解决。但弊端就是用户消息没有进行加密处理，云存储管理员可以访问甚至获得用户的数据，这样给用户带来了很大的安全隐患。因此，目前部分云存储中心采用密文存储方式对用户数据进行保护防止用户隐私泄露的风险。但是同样也面临问题，如用户怎样在云服务器搜索后能找到想要的密文数据，且不在搜索过程中泄露数据信息内容，并且加密操作破坏了原先明文数据的值以及大小关系，其不再具有可供检索的语义和统计特性。为了解决这些问题，可搜索的加密技术应运而生，并引起了人们的广泛关注和大量研究。

Perrig 等人[1]率先提出可搜索加密技术的概念，正如字面所体现的那样，此技术不仅能实现加密操作，防止用户数据隐私的泄露，还能通过密文的搜索，具有很好的应用行和适应性。但是存在的不足就是数据搜索者只能检索自己事先存在云上的密文数据，也就是数据只能被唯一用户检索，并不能达到数据共享。

2004 年 Boneh 等人[2]针对在邮件系统中，搜索带有关键词的邮件场景下采用基于身份的加密体制设计出了一套公钥可搜索加密方案（PEKS）。之后 Dong 等人[3]又在此基础上实现了对关键词可以实现“与”操作的公钥可搜索加密方案。2011 年 Cao 等人[4]又提出了可以实现多关键词检索的公钥可搜索加密方案。但是这些方案的通信模式都是“一对一”[5]的，即加密数据的面

收稿日期：2017-12-19；**修回日期：**2018-02-11

作者简介：许盛伟（1976-），男，江西吉安人，副教授，博士，主要研究方向为网络空间安全密码技术应用（2391651513@qq.com）；王荣荣（1991-），女，山东临沂人，硕士研究生，主要研究方向为公钥密码应用；赵海（1991-），男，山西大同人，硕士研究生，主要研究方向为公钥密码应用.

向检索对象只能是唯一用户。

为了解决以上的数据共享问题，提高检索效率，减少多次加密代价，让加密数据让更多的用户搜索，研究者开始从基于属性的加密（ABE）体制中寻找突破点。ABE 是在 2006 年由 Sahai 等人[6]率先提出来的。它不同于传统的基于身份（IBE）加密体制，它比基于身份的加密体制应用性更强，突破了传统的“一对一”通信方式，即能够实现数据只加密一次就可以被多个用户进行搜索。ABE 的加密方式不再依赖于身份，而是依赖于用户属性和访问策略，并在此基础上提出了两种 ABE 加密体制，分别为 CP-ABE（密文策略的属性基加密机制）和 KP-ABE（密钥策略的属性基加密机制）。CP-ABE 的密文是通过访问策略（或称访问结构）进行加密的，用户私钥是通过用户属性来生成的；KP-ABE 是与 CP-ABE 正好相反的过程，它的密文是通过用户属性来进行加密,用户密钥是通过访问策略生成。显然，两种加密体制可以根据需求适用于不同的应用场景，CP-ABE 加密体制适用于“过滤”用户的场景，即数据拥有者（DO）如果只想让具有某些属性的用户解密数据，那就设计一个策略对数据进行加密，只有满足这个策略的用户才能解密数据，不满足此策略的用户全都无法解密数据,即只有授权用户才能搜索到授权允许访问的信息[7]；KP-ABE 是用户用策略来生成私钥[8]，凡是使用满足此策略的属性进行加密的数据，都可以到达此用户这来进行解密，达到了“过滤”数据的目的。

2014 年李双等人[9]通过借鉴 CP-ABE 体制的加密特性，首次提出了基于属性的可搜索加密方案，并设计出了具体算法以及安全分析，解决了加密数据可被多方搜索的难题，提高了检索效率，特别适用于云服务器上数据的检索。但是存在的问题就是访问策略的暴露，在此方案中，服务器是可以获得密文加密时的访问策略的。有时不仅加密数据含有重要信息，访问策略中也可以提取出好多机密信息，尤其是军方或者金融等敏感领域的应用，一旦从访问策略中提取出敏感数据，将会造成不可估量的损失。

为达到隐藏访问策略，文献[10~11]都设计出了隐藏部分访问策略的 ABE 加密方案，文献[12]提出了一种在素数阶上完全隐藏访问策略的 CP-ABE 加密体制，同时保护了数据和访问策略的安全性。所以，通过文献[12]的隐藏策略思想，本文设计出一种在素数阶上完全隐藏策略的基于属性可搜索方案，并给出了具体算法构造，安全性分析和性能分析，不仅实现了数据共享，提高了检索效率，还保证了访问策略的机密信息不被泄露。

1 基础知识

1.1 符号说明

本文使用的符号如表 1 所示。

1.2 定义

定义 1 双线性群。

设 p,q 是素数，G_1,G_2 分别是阶为 p,q 的乘法循环群，双线性对映射 $e:G_1\times G_1\rightarrow G_2$。如果映射 e 满足下述性质：

a）双线性

对于任意的 $a,b\in Z_p$ 和 $x,y\in G_1$ 都有

$$e(x^a,y^b)=e(x,y)^{ab}。$$

对于任意的 $x_1,x_2,y\in G_1$ 有

$$e(x_1x_2,y)=e(x_1,y)e(x_2,y)。$$

b）非退化性

存在 $x,y\in G_1$ 使得 $e(x,y)\neq 1$，其中 1 是 G_2 的单位。

c）可计算性

存在有效的多项式时间算法对任意的 $x,y\in G_1$，计算 $e(x,y)$ 的值。

表 1 符号说明

符号	含义
G_1	生成元为 g，阶数为素数 P 的双线性群
$e:G_1\times G_1\rightarrow G_2$	一个双线性映射，G_1,G_2 是乘法循环群。
$H_1:\{0,1\}^*\rightarrow G_1$	哈希函数，把任何属性描述为一个二进制的字符串，然后映射到 G_1 中的一个元素
$H_2:G_2\rightarrow G_2$	哈希函数
CT	密文集合
U	属性集合
Υ	访问策略集合
$T_{w'}$	关联于 w' 的搜索陷门

定义 2 BDH：双线性 Diffle-Hellman 问题。

一个双线性映射：$e:G_1\times G_1\rightarrow G_2$，其中随机数 $a,b,c\in Z_p^*$，给定一个四元组 (g,g^a,g^b,g^c)，计算 $e(g,g)^{abc}\in G_2$。

定义 3 DBDH：判定双线性 Diffle-Hellman 问题。

一个双线性映射：$e:G_1\times G_1\rightarrow G_2$，其中随机数 $a,b,c\in Z_p^*$，给定一个五元组 $(g,g^a,g^b,g^c,r),r\in G_2$，判定是否 $e(g,g)^{abc}=r$。

1.3 属性及访问策略定义

在给出方案之前，先描述方案的各部分定义如下：属性全集 $A=\{A_1,A_2,......,A_n\}$，且 $|A|=n$ 表示全部属性个数。A_i 的可能取值集为 $V_i=\{v_{i,1},v_{i,2},......,v_{i,l_i}\}$。用户的属性集为 $U=\{U_1,U_2,......,U_n\},U_i\in A_i$。为用户的每一个属性设置一个标记，记为 $k[i]$，取值有 0 和 1。若 $k[i]=1$，表示用户拥有此属性且 $U_i\subseteq V_i$；若 $k[i]=0$，表示用户并不具有此属性。访问策略表示为 $\Upsilon=\{\Upsilon_1,\Upsilon_2,......,\Upsilon_n\}$，$\Upsilon\subseteq A$。同理，在生成访问策略时，为每个属性 A_i 设置一个标记，记为 $k[i]$，取值有 $1,0,*$。若 $k[i]=1$，表示下表为 i 的属性“必须有”；若 $k[i]=0$，表示下表为 i 的属性“必须没有”；若 $k[i]=*$，表示此属性“无关紧要”，可有可无。在访问策略中，所有下标为（$1,2,...i....,n$）的属性之间用“与”进行连接，同一属性不同的取值之间用“或”进行连接。

给定属性集合 $U=\{U_1,U_2,\ldots\ldots,U_n\}$ 和访问策略 $\Upsilon=\{\Upsilon_1,\Upsilon_2,\ldots\ldots,\Upsilon_n\}$，若用户属性满足访问策略，则必须满足：访问策略中 $k[i]=1$ 的属性 Υ_i，其对应的属性 U_i 的标记也要满足 $k[i]=1$；访问策略中 $k[i]=0$ 的属性 Υ_i，其对应的用户属性 U_i 的标记必须也为 $k[i]=0$。只有这两个条件同时满足，才能称用户属性满足访问策略。

1.4　选择关键词明文的不可区分性安全

在阐明此定义之前，首先定义在选择集合模型下攻击游戏：

a）初始化。敌手选择它想攻击的属性集，成为挑战属性集，并将此属性集发送给挑战者。挑战者运行系统初始化算法，并将所得的公共参数发送给敌手。

b）阶段一。敌手根据选定的访问策略进行门限查询，但是要求是敌手想攻击的属性集（挑战属性集）是不满足这些访问策略的，敌手可以任意选择关键词进行门限查询。

c）阶段二。挑战阶段。敌手随意选择两个不同的关键词 w_0,w_1 发送给挑战者，挑战者随机选择其中的一个 w_b（$b\in\{0,1\}$）进行加密，并将加密结果告知敌手。

d）阶段三。重复阶段一的操作，敌手继续选择关键词进行门限查询，但是要求选定的关键字 $w\notin\{w_0,w_1\}$。

e）阶段四。最后敌手输出猜测值 b'，若 $b'=b$，则敌手猜测正确获胜，所以敌手在整个游戏中的攻击优势为 $Adv=|pr[b'=b]-1/2|$。

所以在攻击游戏下，若敌手在多项式时间内的攻击优势 Adv 是忽略不计的，那就可以称此方案是在选择集合模型下是安全的。

2　完全隐藏策略的基于属性可搜索加密方案算法构造及分析

2.1　方案算法构造

本文将构造一种隐藏访问策略的 KP-ATT-PEKS（密钥策略的基于属性可搜索加密方案）。具体算法如下：

a）$Setup(n)\to(puk,msk)$。

运行系统初始化算法，输入属性集个数 n。G_1 是一个阶为素数 P，生成元为 g 的双线性群且存在双线性映射 $e:G_1\times G_1\to G_2$，在群 G_1 中任取 $\alpha,\beta\in Z_p^*$ 并随机选取 $t_{i,j}\in Z_p^*$，$i=1,2,\ldots\ldots,n$；$j=1,2,\ldots\ldots,l_i$。输出为公共参数以及主密钥，分别为

$$pub=<e,p,g,\{T_{i,j}\}_{i=1,2,\ldots,n}^{j=1,2,\ldots,l_i},g_0,g_1,Y>$$

其中　$T_{i,j}=g^{t_{i,j}}\in G_1,g_0=g^{\alpha},g_1=g^{\beta},Y=e(g,g)^{\alpha}$，

$$msk=<\alpha,\beta,\{t_{i,j}\}_{i=1,2,\ldots,n}^{j=1,2,\ldots,l_i}>。$$

b）$KeyGen(pub,msk,\Upsilon)\to sk$。

输入为公共参数 pub、主密钥 msk，以及访问策略 $\Upsilon=\{\Upsilon_1,\Upsilon_2,\ldots\ldots,\Upsilon_n\}$，权威中心随机选择 $r\in Z_p^*$，所以定义：

$$\tilde{D}=g^{\alpha-r},D_{i,j}=\begin{cases}g^{\frac{r}{t_{i,j}}},k[i]=1\\ g^{\frac{r}{t_{i,j}+\beta}},k[i]=0\\ g^{\frac{r}{t_{i,j}+\beta}},k[i]=*\end{cases}$$

所以，输出私钥为：

$$sk=<\tilde{D},\{D_{i,j}\mid i\in(1,2,\ldots..n),j\in(1,2,\ldots..l_i)\}>。$$

c）$Enctypt(U,w)\to CT$。

输入属性列表 $U=\{U_1,U_2,\ldots\ldots,U_n\}$ 和关键词 w，数据拥有者选择 $s_i,r_i,v_i\in Z_p^*$，且 $S=\sum_{i=1}^{n}s_i+r_i+v_i$，然后计算 $C_0=H_2(t)e(g,g)^{\alpha s}$。其中 $t=e(H_1(w),g_0^s)$，以及

$$\tilde{C}=g^{s},(C_{i,j,1},C_{i,j,2})=\begin{cases}(T_{ij}^{s_i},(T_{ij}\cdot g^{\beta})^{v_i}),k[i]=1\\ T_{ij}^{s_i},(T_{ij}\cdot g^{\beta})^{r_i}),k[i]=0\end{cases}$$

所以可得密文为：$CT=<C_0,\tilde{C},\{C_{i,j,1},C_{i,j,2}\}_{i=1,2,\ldots,n}^{j=1,2,\ldots,l_i}>$

d）$Trapdoor(sk,w')\to T_{w'}$。

输入私钥和要搜索的关键词，生成搜索陷门 $T_{w'}$ 并输出。

其中：　$T_{w'}=[N,X,F]=<H_1^{\alpha}(w'),\tilde{D},\{D_{i,j}\}_{i=1,2,\ldots,n}^{j=1,2,\ldots,l_i}>$

e）$Test(T_{w'},CT)\to b$。

此算法在服务器端执行，当服务器收到用户提交的搜索关键词陷门时，会执行此算法与存储的关键词密文进行比较，输出判断值 $b,b\in\{0,1\}$。若 $b=1$，代表搜索陷门与关键词密文对应同一个关键词；否则，不是同一个关键词。具体算法操作步骤如下：

a) 若属性 U_i 和 Υ_i 的标记 $k[i]=1$，且 $U_i=v_{i,t}$ 则 $e(C_{i,j,1},D_{i,j})=e(T_{ij}^{s_i},g^{\frac{r}{t_{ij}}})=e(g,g)^{rs_i}$。

b) 若属性 U_i 的标记 $k[i]=1$，Υ_i 的标记 $k[i]=*$，则 $e(C_{i,j,2},D_{i,j})=e((T_{ij}\cdot g^{\beta})^{v_i},g^{\frac{r}{t_{ij}+\beta}})=e(g,g)^{rv_i}$。

c) 若属性 U_i 的标记 $k[i]=0$，Υ_i 的标记 $k[i]=0$ 或 $*$，则 $e(C_{i,j,2},D_{i,j})=e((T_{ij}\cdot g^{\beta})^{r_i},g^{\frac{r}{t_{ij}+\beta}})=e(g,g)^{rr_i}$。

所以，每一个属性必须满足上述三个条件的任何一个即可，若有属性并不满足上面任何一个条件，那么输出 $b=0$。

当所有属性都属于上述三个条件时，则有

$$\prod_{i=1}^{n}e(g,g)^{rs_i}\cdot e(g,g)^{rv_i}\cdot e(g,g)^{rr_i}=\prod_{i=1}^{n}e(g,g)^{r(s_r+v_i+r_i)}$$

$$=e(g,g)^{r\sum_{i=1}^{n}(s_r+v_i+r_i)}=e(g,g)^{rs}=Q$$

所以，该算法判断 $C_0/(e(\tilde{C},\tilde{D})\cdot Q)$ 是否等于 $H_2(e(T_{m'},\tilde{C}))$，若相等，则输出 $b=1$，否则输出 $b=0$。

2.2　正确性验证

经过上述算法分析，

$$C_0/(e(\tilde{C},\tilde{D})\cdot Q)=C_0/(e(g^s,g^{\alpha-r})\cdot e(g,g)^{rs}) \\ =C_0/e(g,g)^{\alpha s}=H_2(t)$$，

其中 $t=e(H_1(w),g_0^s)$，且

$$H_2(e(T_{m'},\tilde{C}))=H_2(e(H_1^{\alpha}(w'),g^s))=H_2(e(H_1(w'),g)^{\alpha s})$$

所以，若两者相等，则必有 $w=w'$。即搜索门限和关键词密文对应同一个关键词，且属性集满足访问策略。

3　方案分析

3.1　安全性分析

1）抗攻击性

分析本方案的抗攻击性，本文通过分析本方案在基于属性集合模型攻击下是安全的，最终规约到求解 BDH 问题。根据文献[9]给出的定理，也可以对本文方案作出如下定理：假设 BDH 问题在群 G_1 上是难解的，那么本方案在基于属性集合模型下可以达到抗攻击性安全。现证明如下：

证明　假设存在一个时间多项式算法 A 在基于属性集合的模型下以概率优势 ε_1 可攻击隐藏访问策略的基于属性可搜索加密方案，构建算法 B 以 $\varepsilon \geq \frac{\varepsilon_1}{2}$ 的优势可以求解 DBDH 问题，以 $\varepsilon \geq \frac{\varepsilon_1}{eq_{H_2}q_T}$ 的优势可以求解 BDH 问题。

设 G_1 为生成元为 g 的乘法循环群，且 $u_1=g^a,u_2=g^b,u_3=g^c\in G_1$ 是算法 B 的已知条件，算法 B 的目标是得到 $v=e(g,g)^{abc}\in G_2$ 即解决 BDH 困难问题。现模拟算法 B 为挑战者，算法 A 为敌手，他们之间的攻击游戏如下：

初始化：敌手选择属性集 $U=(U_1,U_2,\ldots U_n)$ 并告知挑战者 B，挑战者运行系统初始化算法，设置公共参数：$g_1=g^a,g_2=g^b,t_{ij}\in Z_p^*$ 是随机选择的。

第一阶段：敌手 A 问询挑战属性集不满足的访问策略所生成的密钥。

a)若属性集 U 满足访问策略，则以下三点成立：

① Υ_i 的 $k[i]=1$，U_i 的 $k[i]=1$

② Υ_i 的 $k[i]=0$，U_i 的 $k[i]=0$

③ 3 Υ_i 的 $k[i]=*$，U_i 的 $k[i]=0$ 或 1

b)若属性集 U 不满足访问策略，则以下两点成立：

① Υ_i 的 $k[i]=1$，U_i 的 $k[i]=0$

② Υ_i 的 $k[i]=0$，U_i 的 $k[i]=1$

所以当下表为 i 的属性属于情况 1 时，生成密钥为

$$\tilde{D}=g^{a-r},D_{i,j}=\begin{cases} g^{\frac{r}{t_{i,j}}},k[i]=1 \\ g^{\frac{r}{t_{i,j}+b}},k[i]=0 \\ g^{\frac{r}{t_{i,j}+b}},k[i]=* \end{cases}$$

所以，当下表为 i 的属性属于情况 2 时，生成密钥为

$$\tilde{D}=g^{a-r'},D_{i,j}=\begin{cases} g^{\frac{r'}{t_{i,j}}},k[i]=1 \\ g^{\frac{r'}{t_{i,j}+b}},k[i]=0 \end{cases}$$

所以，综上合并以上两种情况，令 $r=r'$，则可以得到

$$\tilde{D}=g^{a-r},D_{i,j}=\begin{cases} g^{\frac{r}{t_{i,j}}},k[i]=1 \\ g^{\frac{r}{t_{i,j}+b}},k[i]=0 \\ g^{\frac{r}{t_{i,j}+b}},k[i]=* \end{cases}$$

所以算法 B 可以构造具有访问策略 Υ 的密钥。

阶段二：敌手向随机预言机 H_1,H_2 进行关键词 w 陷门值 T_w 的查询，过程同文献[2]。

阶段三：敌手进行挑战，任选两个关键词 w_1,w_2 且作为挑战关键词发送给挑战者 B，B 随机选择 $b\in\{0,1\}$，生成关键词密文 C_b 发送给敌手 A，其中：

$$C_b=<C_0,\tilde{C},\{C_{i,j,1},C_{i,j,2}\}|_{i=1,2,\ldots,n}^{j=1,2,\ldots,l_i}> \\ =<JZ,g^c,\{C_{i,j,1},C_{i,j,2}\}|_{i=1,2,\ldots,n}^{j=1,2,\ldots,l_i}>$$

且 $J=H_2(t)=H_2(e(H_1(w_b),g_0^c),z=e(g,g)^{ac}$。

阶段四：重复阶段一的操作，敌手 A 可以询问除关键词 w_0,w_1 以外的关键词所对应的的陷门。

阶段五：挑战者 B 根据敌手 A 的判断结果而输出结果，若 A 的猜测为 b'，当 $b'=b$ 时，挑战者得到 $c'=1$；若 $b'\neq b$，得到 $c'=0$。所以算法 B 求解 DBDH 问题的概率为 $\varepsilon \geq \frac{\varepsilon_1}{2}$。又因为 $\tilde{C}=g^c$，$J=H_2(t)=H_2(e(H_1(w_b),g_0^c),z=e(g,g)^{ac}$，参考文献[2]中的分析，根据随机预言机 H_2 的查询和 H_2-list 列表中保留的查询数列 (t,v)，$t=e(H_1(w_b),g^{ac})=e(g,g)^{ac(b+a_b)},v=H_2(t)$，故有 $\frac{t}{e(g^a,g^c)^{a_b}}=e(g,g)^{abc}$。并且计算出 $e(g,g)^{abc}$ 的概率 $\varepsilon \geq \frac{\varepsilon_1}{eq_{H_2}q_T}$[2]。

综上，在随机预言机 H_1,H_2 下，若存在攻击隐藏访问策略的基于属性可搜索加密方案的概率为 ε_1，那么经过上述证明之后，得到存在求解 G_1 中 DBDH 问题的优势概率为 $\varepsilon \geq \frac{\varepsilon_1}{2}$，在 DBDH 可解的情况下，求解 BDH 问题的概率优势为 $\varepsilon \geq \frac{\varepsilon_1}{eq_{H_2}q_T}$，其中：$q_{H_1},q_{H_2}$ 分别代表 H_1,H_2 的询问次数；q_T 为陷门的询问次数。

2）隐藏访问策略

在传统的 ABE 方案中，访问策略是保存在密文当中的，随密文一同上传到服务器的，在文献[9]中基于属性的可搜索加密

方案中，服务器也是可以获得访问策略的，以便进行 $Test(T_{w'}, CT) \to b$ 操作。所以，在好奇且不可信赖的服务器上，它是会获得访问策略并从访问策略中提取信息，从而造成信息的泄露，但是本方案是完全隐藏访问策略的，服务器不会获得访问策略，从而不会对访问策略中的信息造成泄露。

3）索引及关键词的安全性

在本方案中，索引是经过加密上传到服务器的，所以服务器以及攻击者除了获得密文索引之外，是得不到任何索引的具体明文信息的，从而保证了索引的安全性。用户在提交关键词陷门时，由于关键词是经过哈希函数进行加密的，所以服务器对陷门中的关键词也是一无所知的。

3.2 性能分析

将本方案与同样是基于公钥加密索引的 PEKS[2]、ATT-PEKS[9]（基于属性的可搜索加密）方案在运算量以及实现功能上进行了比较。运算量是对方案各部分算法的运算次数进行统计的，其中 P 代表双线性运算，E 代表指数运算，H 代表哈希运算，属性集的属性个数为 n。在算法列中 Crypt 代表加密操作，Test 代表服务器上的判断操作（判断索引密文与关键词陷门是否匹配），Trapdoor 代表生成陷门操作，Setup 代表初始化算法，KeyGen 代表生成密钥操作，最后两列为各方案的功能比较，其中加密数据共享代表数据密文可以让多用户进行搜索。其统计如表 2 所示。

表 2　各方案运算量及功能统计

算法	功能			
	操作	PEKS	ATT-PEKS	本方案
Crypt	P	1	2	2
	E	2	3+n	3+2n
	H	2	2	2
Test	P	1	1	1
	E	0	0	0
	H	1	1	1
Teapdoor	P	0	0	0
	E	0	1	1
	H	1	1	1
Setup	P	0	0	1
	E	2	2	2
	H	0	0	0
KeyGen	P	0	0	0
	E	2	$O(n^n)$	n+1
	H	0	0	0
加密数据共享	P E H	×	√	√
隐藏访问策略	P E H	×	×	√

从表中可以看出，PEKS 的运算量最少，但是它是最先出现的公钥可搜索加密方案，当需要发送给多个用户时，需要针对每个用户的公钥以此来加密生成数字信封；当用户量较多时，需要进行多次加密，无法实现只加密一次的数据共享，而且用户公钥存储是一个很大的问题，还要进行公钥证书的认证，以防窜改。本方案与 ATT-PEKS 方案相比较发现，本方案在加密（Crypt）操作上会有运算次数 n 的略微增加，但是 ATT-PEKS 方案却在 KeyGen 操作上运算量达到了 $O(n^n)$ 级别，远大于本方案的运算量，并且还不具有隐藏访问策略的功能。所以，综上运算量和功能这两方面的比较，会发现本方案不仅实现了加密数据共享和隐藏访问策略，还具有较少的运算量。

4　结束语

本文首次提出了具有完全隐藏访问策略的基于属性可搜索加密方案的算法构造设计，并对其安全性以及性能进行了分析，证明了本方案是在属性集合下可抗攻击性的，还保证了访问策略、索引和关键词的机密性，打破了以往可搜索加密方案中访问策略暴露的限制。在安全的前提下，本方案还能够实现加密数据能被多方搜索，不同用户使用不同的访问策略可以获得与自己相匹配的加密数据，实现了数据的共享，提高了检索效率，扩展了应用性。

参考文献：

[1] Perrig A, Wagner D, Song D X. Practical techniques for searches on encrypted data [C]// Proc of IEEE Symposium on Security & Privacy. 2000.

[2] Boneh D, Crescenzo G D, Ostrovsky R, *et al.* Public key encryption with keyword search [M]// Advances in Cryptology-EUROCRYPT 2004. Berlin: Springer, 2004: 506-522.

[3] Dong J P, Kim K, Lee P J. Public key encryption with conjunctive field keyword search [C]// Proc of International Conference on Information Security Applications. [S. l.] : Springer-Verlag, 2004: 73-86.

[4] Cao N, Wang C, Li M, *et al.* Privacy-preserving multi-keyword ranked search over encrypted cloud data [J]. IEEE Trans on Parallel & Distributed Systems, 2011, 25 (1): 222-233.

[5] 马明军，杨亚涛，王培东，等. 基于属性的可认证搜索加密方案 [J]. 计算机工程与设计, 2016, 37 (2): 358-362.

[6] Sahai A, Waters B. Fuzzy identity-based encryption [C]// Lecture Notes in Computer Science. 2005: 457-473.

[7] 房梁，殷丽华，郭云川，等. 基于属性的访问控制关键技术研究综述 [J]. 计算机学报, 2017, 40 (7): 1680-1698.

[8] 田野，彭彦彬，杨玉丽，等. 无线体域网中基于属性加密的数据访问控制方案 [J]. 计算机应用研究, 2015, 32 (7): 2163-2167.

[9] 李双，徐茂智. 基于属性的可搜索加密方案 [J]. 计算机学报, 2014 (5): 1017-1024.

[10] 王海斌，陈少真. 隐藏访问策略的基于属性加密方案 [J]. 电子与信息学报, 2012, 34 (2): 457-461.

[11] 解理，任艳丽. 隐藏访问策略的高效基于属性加密方案 [J]. 西安电子科技大学学报: 自然科学版, 2015, 42 (3): 97-102.

[12] 刘雪艳，郑等凤. 基于素数群完全隐藏访问策略的 CP-ABE 方案 [J]. 计算机工程, 2016, 42 (10): 140-145.